Testimony
House Committee on Homeland Security
Subcommittee on Emerging Threats, Cybersecurity and Science and Technology
Addressing the Nation's Cybersecurity Challenges:
Reducing Vulnerabilities Requires Strategic Investment and Immediate Action
James A. Lewis
Center for Strategic and International Studies
April 25, 2007

I would like to thank the Committee for the opportunity to testify. Cybersecurity is one of those problems that seem to be intractable. It is also a problem that, in the past, seemed to attract exaggeration and hyperbole. The combination is not ideal for creating effective policies, in part because the blend of intractability and exaggeration can create indifference.

One way to overcome this indifference is to put cyber security in the right context. For Federal networks, the context for cybersecurity involves two sets of risk. The first involves espionage. The second involves the potential interruption of the delivery of federal services.

I will focus my remarks today on the security of Federal networks. Most networks are, of course, connected in some way, and the security of Federal networks has serious implications for homeland security in both continuity of operations and for critical infrastructure. In addition, measures that improve the security of Federal networks will also benefit private sector networks. My own view is that the security of federal networks is the most serious cybersecurity challenge we face, more serious than critical infrastructure or cybercrime.

The most important of these risks involves espionage. Cybersecurity is at this time primarily a spy story. Cyber-espionage poses the greatest current threat. Hacking is the extension of signals intelligence into new and untrammeled areas. Foreign intelligence agencies must weep with joy when they contemplate U.S. government networks. We have thoughtfully placed sensitive information on these networks and then failed to secure them adequately. This is not a hypothetical problem. The last twenty years have seen an unparalleled looting of U.S. government's databases.

The reliance upon information technology has changed the nature of espionage. Information is more valuable. Nations will use the traditional means of espionage (infiltration and recruitment) to obtain access to information, but information technologies have created a gigantic new opportunity. Hacking into computer networks (which are vulnerable and likely to remain so for years) provides new, low cost and low risk opportunities for espionage. Eight or nine countries have the advanced technical skills needed for these operations and smaller countries can hire hackers from the criminal world.

Conflict in cyberspace is clandestine, so it can be difficult to assess intentions and risks. It is easier to assess the vulnerability of U.S. systems and the consequences of an information attack. U.S. networks are very vulnerable. Even highly sensitive networks used for command and control or intelligence are not invulnerable. From an intelligence perspective, several nations, have exploited the vulnerabilities of U.S. government networks to gain valuable information. These foreign intelligence efforts and the inadequate U.S. response have damaged national security.

You heard last week about some of the problems that agencies face. Their testimony highlights that securing federal networks from cyber attack is one of the greatest challenges facing the United States, and that the scope of the challenge and the threat to national security

are difficult to appreciate fully. Several incidents that occurred in the past few months help to illustrate the scale of the problem. In December and January 2006, for example, the Naval War College, the National Defense University, and other DOD facilities had to take computer networks offline after a foreign entity infected them with spyware. Before the last shuttle launch, NASA had to block e-mail attachments to avoid outsider attempts to gain access before a Shuttle launch. And as you heard last week, the Department of Commerce had to all of the computers at the Bureau of Industry and Security offline after they were hacked and infected with spyware.

The threat of the disruption of services remains hypothetical. Unlike cyber-espionage, which is occurring on a daily basis, there has been no disruption of services. We should not take much comfort from this, however. If an opponent can hack in to federal networks to steal information, they are likely to also be able to hack in to implant malicious software that could be triggered in a crisis to disrupt services or to scramble data. We should assume that many of our potential opponents are exploring informational attacks to disrupt U.S. government services and databases.

It is easy to overstate the effect of this disruption, but we should assume that several of our potential opponents are exploring disruptive strategies as part of their planning for information warfare. Increasing uncertainty in the mind of an opponent degrades that opponent's effectiveness. This is a classic intelligence strategy, and cyber attacks on an opponent's information systems provide new and expanded means to execute it. Denial and deception can make opponents certain that they know what is happening when, in fact, what they believe is wrong, or it can make them unsure that they know what is happening. Finding ways to inject false information into the planning and decision processes of an opponent, or manipulating information that is already in that system to make it untrustworthy, can provide military advantage. We should assume that in the event of a conflict, our opponents would pursue an informational strategy that seeks to expand uncertainty and confusion instead of attempting to unleash an 'electronic Pearl Harbors' that offers only uncertain results.

This litany of threats and risks might lead some to ask if the U.S. was better off before it depended so heavily on computer networks. The answer to that question is no. The benefits to the U.S. that come from the greater use of networks and computers outweigh the damage from poor cybersecurity. It is better to have networks than to be without them, and the use of computer networks provides the U.S an advantage in its economy and its military operations. However, the porousness of our Federal networks erodes those benefits. Greater attention to cybersecurity would increase the benefits our nation gains from networks and close off an avenue of asymmetric advantage to our opponents.

There have been serious efforts in the national security community to make their networks more secure. Our most sensitive military and intelligence functions are probably secure. Some civil crucial networks are more secure – much attention has been paid to Fedwire, the Federal Reserves electronic funds transfer system, for example. But, as you heard last week, many agency networks remain poorly secured, and it is safe to say that reams of diplomatic, scientific, administrative and defense industrial information at the various agencies have not been adequately secured. In looking at the security of Federal networks, it is fair to say that while the U.S. is better off than it was five years ago or ten years ago, the improvement has been unevenly distributed among agencies. Some are secure, most are not.

Additionally, some efforts to improve cybersecurity have not had the benefits we expected. It is quite possible for our opponents to hack a computer running software that has Common

Criteria certification, on a network that has met the requirements of ISO 19779, at an agency that has gotten good marks on FISMA. In other words, you can meet all the formal requirements and still be vulnerable.

This is also a dynamic situation, dynamic in the sense that attacks are continuous and continuously changing. We should applaud those agencies that have, after some months, discovered their networks have been hacked and have taken steps to undo that hack, but our next question should be, "and now what are you doing." Attacks on Federal networks are continuous, and fixing one problem does not mean that we have checked the box and can turn our attention elsewhere.

How doe we change this situation? There is no silver bullet, no single program or effort that will remedy this problem. Increased funding will not improve security. The Federal government is a complex enterprise, with thousands of networks and hundreds of thousands of computers. No single agency has control of this collection of networks. Some Federal networks are among the most secure in the world, although even these are not immune from attack. Others are routinely penetrated. Some systems use the most advanced technologies. Others are legacy systems, running programs that may date back many years and which, for all practical purposes, cannot be secured.

Making networks more secure is a large and complex problem. The core of the problem is organizational. Although it has been more than a decade since the Marsh report on the risks posed by cyber attack to critical infrastructure, and although there has been progress, the federal government is still disorganized when it comes to cyber security. The Department of Homeland Security, the Federal CIO Council, and the Office of Management and Budget all play a role in securing federal networks. But cybersecurity remains a low priority and an afterthought for many agencies. The Federal response to cybersecurity remains largely ad hoc and dispersed.

The need for a better strategy complements the need for better organization. There is, of course, a national cyber strategy from 2003, but that strategy it is now outdated. It shifted too much of the burden for security to the private sector and did not resolve key issues regarding responsibility within the government. A new, comprehensive cyber security strategy for the Federal government would need to include a number of complementary measures to reduce vulnerabilities. The following paragraphs provide a brief outline of some of the major elements of this approach.

Rationalizing and streamlining governmental processes for improving cybersecurity is essential. There are too many interagency groups and committees working on the same problem, often with the same people, and few of them have the authority to make any real progress. The U.S. does not need a new White House cyber czar, but it does need to do more to direct and coordinate efforts by the various agencies. The recent creation of a cybersecurity Policy Coordinating Committee at the National Security Council is an important first step.

Second, the U.S. can do more in the area of improving agency practices when it comes to networks security. Cybersecurity is still a third tier priority at many agencies. If gangs of foreigners broke into the State or Commerce Departments and carried off dozens of file cabinets, there would be a crisis. When the same thing happens in cyberspace, we shrug it off as another of those annoying computer glitches we must live with. Agencies need to be held

accountable for breaches. Our current approach is to treat losses of information through inadequate security as something that is separate from the performance of senior officials.

The separation between the national security agencies and civilian agencies needs to be reduced. The national security agencies do better at security, but there is no good mechanism for sharing their expertise and experience with the civilian agencies. Developing better ways to coordinate network security efforts between agencies and to identify, share and enforce best practices for federal network security across agencies would reduce risk and damage.

Better identity management would also help improve cybersecurity. As long as it is easy to impersonate someone else on the internet, networks will never be secure. In this, initiatives like HSPD 12 and the Real ID Act offer the possibility to reduce risk. HSPD-12 mandated strong identity procedures and credential for the Federal government and its contractors HSPD-12, along with Real ID, lay the foundation for robust authentication of identity. Much remains to be done, but the U.S. has begun to adjust how it manages identities to fit digital technologies and this will improve security.

One new area the government can begin to address is how to improve software assurance. This means creating processes for transparency, evaluation and coordination where the government determines how much it can trust the software it buys. It might be useful to consider when the U.S. faced a similar problem and what it did about it. This story has an unlikely hero - Herbert Hoover. Hoover may have been a terrible or unlucky President, but he was a great Secretary of Commerce. One of the things he did in the 1920s as Secretary of Commerce was call a number of leading companies from different sectors - automobiles, electrical equipment and so on, to the Commerce Department and say that they had to come up with a means to improve quality and interoperability in their products. This was the start of the industry-led standards process.

We need something similar to happen for security and software production. There are existing standards bodies for software. These standards are aimed at products – how they perform and how they interoperate. The U.S. does not need to duplicate them. What we need is a new means for understanding how to produce software in ways that can assure security.

CSIS recently did a study that looked at how some of the larger IT companies write software. We found considerable attention to security among the companies, and that each company had a set of ‘best practices’ for software assurance that make their products more secure. We also found that each company’s best practices were somewhat different, and that these practices were sometimes unevenly applied.

Finding a way to extend commercial best practices for assurance would benefit both Federal networks and the private sector. The procedures companies use as part of their software production process internal reviews and testing for performance and security, external testing and red-teaming, and the use of software review tools (some commercial, some proprietary and developed by the software company itself) to find vulnerabilities or errors. These practices offer the building blocks for an approach that could reduce vulnerabilities.

The key to these new processes should be to build upon what is already done within the private sector when it comes to software. Software producers realize the importance their customers place on assurance and security and have adjusted their internal procedures to meet this market demand. While there is much commonality and overlap in what companies do,

each company approaches the issues of assurance and security somewhat differently. From these differences, we can extract best practices and requirements that will address, as part of a larger solution set, the risks posed by foreign involvement in software production.

Please note that I am saying best practices, not standards. An attempt to have the government mandate standards for software production and then enforce them would damage the American economy without producing any benefit for security. So new regulations, new government standards are not the solution. However, the government could encourage industry to use best practices for making secure software by linking practices to its acquisitions policies. If the Federal government gave preference in its acquisitions to software that was developed with trustworthy processes, it would provide an incentive that would benefit both the federal and the commercial markets.

Companies are making serious efforts to improve software assurance, but the government needs to be able to understand and guide those efforts. Traditional approaches to governance – command and control or heavy regulation – would increase assurance at an unacceptable cost. The U.S. needs news ways to let the government and the private sector work together to develop some generalized set of best practices for software production, and the Departments of Defense and Homeland Security are involved in some interesting work in this area.

Continued attention to continuity of operations and continuity of government can mitigate the risk of disruption of federal services. As part of a Federal cybersecurity strategy, this would entail measures to keep networks operating at some minimal level and to provide continued access to data. This is an area where there has also been some progress.

Finally, the U.S. can take steps to keep itself at the forefront of technology. This goes beyond simply funding more cyber-security research. Overall, the U.S. invests more than other nations in research, but this investment may not be enough, in an era of increased international competition, to preserve leadership. Federal investment in the research that undergirds technological innovation offers tremendous returns for both the economy and for security. Innovation makes life more difficult for opponents. Measures that improve the climate for innovation in the U.S. also help build a skilled domestic workforce.

These steps - better federal organization, best practices for coding combined with acquisitions, better identity management, attention to continuity of government and renewed support for technological leadership - can form a coherent strategy for improving the security of Federal networks and cybersecurity in general. Being able to articulate a strategy is important, but implementation will always be a challenge. In this, Congressional oversight is critical to this. Without Congress to press senior leadership at Federal agencies to do better, progress will take much longer than would otherwise be the case.

It has been more than twelve years since the U.S. became concerned with the vulnerabilities created by its use of computer networks. There has been some improvement in that time, but not enough. We have an opportunity in the next few years to change this with improved Federal organization and better strategies. Our goal should not be perfect security, but to gain more advantage than our opponents from the use of information technology.

I thank the committee again for the opportunity to testify. I ask that my entire statement be entered into the record, and I will be happy to take your questions.